Do market forces drive fraud?

May 29, 2009

In today's U.S. markets for payment and credit services, have we overshot the mark in keeping personally identifiable information private, thereby lowering the bar to fraudsters?

Providers of credit and payment services traditionally required customers to have a public identity, such as by providing references, allowing the provider to verify the person's identity and creditworthiness before opening an account. This required the potential customer to be socially engaged and sacrifice some privacy to establish a public identity. Some non-Western cultures still look to public personas to help ensure good conduct. Consider **Qifang**, a new Chinese peer-to-peer lending business, which requires potential borrowers to provide not only personal information but also information about family members, thereby raising the penalty for default as it may cause the whole family to "lose face."

U.S. consumers have come to expect instant gratification in their ability to open accounts, obtain credit, and complete payments. Further, they tend to demand privacy and security of their personally identifiable information and want to share the least information that will facilitate the transaction. These market demands may drive payment services providers to impose the least amount of privacy requirements and security risk on their customers to facilitate the most "frictionless" transactions possible. While perhaps inevitable and likely a positive driver of payments innovation, this confluence of market forces may nevertheless increase the vulnerability of payment systems to risks such as those resulting from identity theft and new account fraud—less information is demanded of a legitimate customer, so similarly the hurdles to wrongdoers are lower.

Some thinkers in this arena have applied economic analysis to the trade-offs between privacy, data security, and fraud prevention. Others have advocated re-evaluating entirely how we view privacy, by severing the link between identification information (which should be harmless and public) and privacy, in effect permitting individuals to preempt imposters by making their identity fully public and allowing anyone to verify it easily.

While there is great emphasis on protection of personally identifiable information (driven by law and regulation, consumer demand, fear of reputational impact from data breaches, etc.), as long as such information can be used effectively to perpetrate fraud, risks will persist. As payment providers simultaneously compete for the most user-friendly, hassle-free, fast, private, secure services model, they also may have incentives to require less personally identifiable information. This is less intrusive for their customers and also helps avoid storage of such information. This may drive providers to require the lowest level of information and, as mentioned before, lower the bar for fraudsters as well.

Do these market incentives in effect foster an environment where identity theft and resultant payment frauds can proliferate? If so, how can this problem best be addressed?

*By Clifford S. Stanford, assistant vice president and director of the Retail Payments Risk Forum at the Atlanta Fed*

- May 29, 2009 in
  - identity theft
payments risk

Permalink
Comments